IONA

Orbix®

Release Notes

Version 6.1, December 2003

Making Software Work Together™

Contents

CONTENTS

Orbix 6.1 Release Notes

In this document

This document contains the following sections:

Features Removed

The following feature has been removed in the Orbix 6.1 release:

*   The application server in Orbix E2A Application Server Platform 6.0 is no longer provided in Orbix 6.1. For information on IONA's J2EE offerings, see
    http://www.iona.com/products/j2ee/

CORBA Compliance

Orbix 6.1 complies with the following specifications:

*   CORBA 2.6
*   GIOP 1.2 (default), 1.1, and 1.0
*   C++ Language Mapping (formal/99-07-41)
*   IDL to Java Language Mapping (formal/99-07-53)
*   Object transaction service (OTS) 1.1 and 1.2

New Features

Orbix 6.1 includes the following new features:

- "Connector for Microsoft .NET Framework" on page 2.
- "Bidirectional GIOP" on page 3.
- "Improved Scalability using Java NIO" on page 3.
- "Extended Security Infrastructure including Single Sign On (SSO)" on page 4.
- "Smart Card Support" on page 5.
- "Integration with the Tivoli Enterprise Management System" on page 5.
- "Enhanced Notify Performance" on page 6.
- "New Logging Features" on page 6.

Migrating from Version 5.1 If you are upgrading from earlier versions of Orbix, see *Migrating from 5.1 to 6.1*. This is available at the IONA Documentation home pages (http://www.iona.com/support/docs/orbix/6.1).

Connector for Microsoft .NET Framework

There are two methods available for communicating between application domains:

- Web Services
    - Standards-based
    - Internet friendly
- .NET Remoting
    - Allows use of stateful objects
    - Flexible and extensible allowing different transports and protocols to be used.

The native .NET connector in Orbix 6.1 takes advantage of the extensibility of .NET remoting to allow connectivity to CORBA servers. Other features include:

- Enterprise CORBA scalability for .NET
- Visual Basic, Visual C#, Visual J#, and managed C++ clients can call CORBA and J2EE Servers.
- Standard .NET API, requiring no CORBA knowledge.

- Non-intrusive to existing CORBA systems.
- Security, transaction, load balancing, and fault tolerance features available to a normal Orbix C++ client in Orbix Enterprise.
- .NET connector is available on Windows XP and Windows Server 2003 operating systems.

Bidirectional GIOP

The Orbix 6.1 implementation of bidirectional GIOP has the following features:

- Compliant with the modified bidirectional GIOP approach described in the firewall submission.
- Compatible with GIOP 1.2 (that is, not dependent on GIOP 1.4 NegotiateSession messages).
- De-coupled from IIOP, so that it can be used over arbitrary connection-oriented transports (for example, SHMIOP).
- Supports weak BiDirIds initially.
- Supports bidirectional invocations on legacy Orbix 3.x callback object references in order to facilitate phased migration to Orbix 6.x.

Improved Scalability using Java NIO

J2SE 1.4 introduced "new I/O" APIs to enhance scalability. These allow many connections to be managed with fewer resources (specifically, threads). Performance is better than Java "classic I/O" (CIO) for many concurrently active connections. Java NIO is enabled using a single configuration variable as follows:

```
plugins:atli2_ip:ClassName =
"com.iona.corba.atli2.ip.nio.ORBPlugInImpl"
```

Transports based on CIO are still supported and remain the default.

> **Note:** Java NIO does not yet support either JSSE or multicast. Thus, when IIOP/TLS or EGMIOP protocols are in use, only CIO may be used.

Extended Security Infrastructure including Single Sign On (SSO)

Orbix 6.1 provides the following security features:

Single Sign On Support for C++ and Java Applications Hugely increased security of iS2 user/password deployment where the user/password visibility is restricted to the CORBA Login service, layered above CSIv2. Clients use SSO tokens to talk to server applications. SSO support for both username and password and TLS x.509 client authentication. Allows TLS X.509 clients to talk to servers that demand CSIv2 username/password authentication. The new CORBA Login Server (lives in the same process as existing security service by default). IONA's integration allows CORBA clients to simply be configured to use single sign on with no code changes. Importantly, SSO token expiry and automatic refreshing of SSO tokens handled transparently to the application. Without this, all customer applications would need a large amount of exception handling code.

CFR Authorization Support Administrators have the ability to define ACL for configuration scopes and only authorized users can read/write to sensitive scopes. The hierarchic nature of the Orbix configuration scoping mechanism makes it easy to define ACLs for groups of related applications that share a parent configuration scope. Replication of CFR now supported in iS2 environment. The CFR security model is pluggable.

Sophisticated New ACL Extensions SDK support is now provided for users to write custom Action Analyser plug-ins. You can define an ACL that is based on the *values* of the parameter list. The action analyser plugin determines what resources are actually being accessed. Also, the ACL enforcement mechanism checks that users have the appropriate rights for all these actions. No application code changes are required.

Additionally, extended wildcarding support for ServerNames, interfaces and operations is provided.

IONA Security Framework Features The *Security Guide* contains information about security features that are provided in several IONA products. The following IONA Security Framework features are not currently supported in Orbix 6.1:

- Siteminder adapter
- iS2 clustering

The following IONA Security Framework feature is not included in your Orbix 6.1 Standard or Enterprise license:

- support for developing custom iS2 server adapters

Please contact your IONA account manager or IONA Customer Services for information on how to obtain a license for custom iS2 adaptor support.

Smart Card Support

A smart card is a microprocessor device for cryptographic operations and storing of security keys. Smart cards ensure enhanced security by verifying the card holder and making the whole process tamper-proof, as the private key never leaves token. It is used in conjunction with the SSL/TLS protocol.

Orbix 6.1 TLS Smart Card Usage Smart card setup is vendor-specific. It is compatible with existing IONA security framework, for example, ISF, SSO and it is ART-based. Supported on C++ and Java.

Integration with the Tivoli Enterprise Management System

Huge IT organizations, with hundreds or thousands of servers, many operating systems, and dozens of software vendors in a mission-critical environment require an integrated management system. In an Enterprise Management System (EMS), faults are correlated so that operators find the cause rather than being swamped by the symptoms. It provides a single management console where recovery actions are automated. It also provides a number of useful tools such as Service Level Agreement monitoring, business impact analysis and churn analysis.

IONA's Tivoli integration supports the posting of an event when a server dies, so that recovery actions can be taken automatically. It tracks key server metrics, such as the number of invocations received and the average, maximum, and minimum response times. Also, events can be generated when any of these parameters go out of bounds, and it enables an extensible set of actions to be performed on servers, such as start, stop and restart.

IONA's Tivoli integration is based on a generic architecture for EMS integration. Key metrics are logged by IONA performance logging plug-ins. Log file interpreting utilities are used to analyze the logged data. A relatively small piece of code provides glue to the Tivoli Java APIs. Tivoli APIs enable endors such as IONA to implement WBEM/CIM providers.

See the *IONA Tivoli Integration Guide* for full details on integrating with Tivoli.

Enhanced Notify Performance

Orbix Notification 6.1 performance is double the throughput than that of Application Server Platform Notification 6.0. It provides a similar performance to that of VisiNotify. However, VisiNotify avoids marshalling completely which leads to the following problems:

- Out of compliance with the specification.
- Messages are lost under certain conditions.
- QoS only partially supported.
- Delivery in heterogeneous environments is sometimes impossible.
- Event translation is not supported.
- Subscription interchange not supported.

New Logging Features

Extra Logging Output (enhancement 68078) To aid application debugging, extra logging output has been added to the Orbix locator and node daemon services, specifically in the areas of endpoint cache entries, and process activation and deactivation.

The specific new logging events are:

```
IT_LOCATOR Log Namespace:
   const IT_Logging::EventId NODE_DAEMON_NO_RESPOND         = 115;
   const IT_Logging::EventId ENDPOINT_CACHE_SETUP           = 150;
   const IT_Logging::EventId ENDPOINT_CACHE_ADD_REPLIC      = 151;
   const IT_Logging::EventId ENDPOINT_CACHE_REMOVE_REPLICA  = 152;
   const IT_Logging::EventId ENDPOINT_CACHE_REMOVE_DAEMON_ENTRIES
   = 153;
```

```
IT_NodeDaemon Log Namespace:
    const IT_Logging::EventId PROCESS_SIGNALING   = 17;
    const IT_Logging::EventId PROCESS_STARTED     = 18;
    const IT_Logging::EventId PROCESS_NOT_FOUND   = 19;
    const IT_Logging::EventId PROCESS_NO_RECOVERY = 20;
```

To see these extra logging messages, set the following configuration variable:

```
event_log:filters=["IT_NodeDaemon=*", "IT_LOCATOR=*"];
```

Dynamically reconfigure the Logging Levels for IONA Services (enhancement 68189) It is possible to update the `event_log:filters` setting for a particular server on-the-fly, without having to stop the server in question. To enable this feature, the services must be started in a managed domain. Then, the IONA Management Console can be used to navigate to the individual service and set the logging settings on the service's `event_log:filters` MBean value.

Known Issues

The following known issues exist in Orbix 6.1:

Installation and Configuration
- Installing Orbix Visual Studio wizards.
- Uppercase or mixed case hostnames.
- Using the -background flag on Windows.
- itconfigure does not deploy services on a virtual host.
- itconfigure on SuSE Linux.

Web services
- Web Services Test Client.
- Using the Web Services Registry Manager.

Security
- Creating a Domain with iS2 enabled.
- Performance optimization for TLS servers.
- Important multiple listeners security warning for TLS servers.
- Security service on Windows and Linux.
- Notification service in a secure domain on Linux AS 3.0.
- Unsupported IONA Security Framework features.

Demos
- Codeset_Converter demo on HP-UX.

Installation and Configuration

The installation and configuration issues are as follows:

Installing Orbix Visual Studio wizards

In some cases, the Orbix Visual Studio wizards will not be installed automatically by the installer. See the *Orbix Installation Guide* for instructions on how to manually install these wizards.

Uppercase or mixed case hostnames

Specify lowercase hostnames when configuring Orbix. Using uppercase hostnames, or a mix of lowercase and uppercase hostnames may result in problems.

Using the -background flag on Windows

On Windows, it is not possible to run a service with the `-background` flag if the `principal_sponsor:csi:auth_method_data` is not specified in configuration. If the service must run in the background, it is recommended that a password file is used, and that access to that password file is restricted to `Administrator` only. For example:

```
principal_sponsor:csi:auth_method_data = ["username=Administrator",
"password_file=U:\secure_directory\secret.pwf", "domain=IONA"];
```

itconfigure does not deploy services on a virtual host

`itconfigure` does not deploy services for which the specified host is a virtual host or network interface. This is also applies when the `-multihome` command line option is used.

For example, on a host named `orion` and a second network interface named `orion-virtual`, run `itconfigure` in GUI mode. For all selected services change the default host from `orion` to `orion-virtual`. When you click **Next** on the **Summary** page, `itconfigure` correctly asks the following question:

```
There are no services or demo configuration to deploy on the local
host (orion). Do you want to deploy the services for host
orion-virtual instead?
```

This usually requires that `orion-virtual` host designates the same physical machine as `orion`.

If you click **Yes**, `itconfigure` proceeds to deploy a minimal configuration, but does not deploy the selected services.

The same happens if `itconfigure` is used with the `-multihome orion-virtual` command line option, both in GUI and non-GUI mode.

A patch is available to fix this problem. Please contact support@iona.com for download details.

itconfigure on SuSE Linux

On SuSE Linux Enterprise 8, with JDK1.4.1 used on the KDE desktop, the layout of the controls in the `itconfigure` GUI is incorrect. The font spacing is responsible for this issue.

A patch is available to fix this problem. The patch allows the GUI to automatically resize if the font spacing is wrong. Please contact support@iona.com for download details.

Web Services

The Web services issues are as follows:

Web Services Test Client

Selecting a sample Web service from the **Web Services Test Client** fails with an `unknown protocol` error when used in a fully secure domain.

To test one of the sample Web services, you must generate a Web service client using the **Web Service Builder**, following the steps documented in the 'Build and Run a Secure Client' section of the 'Securing Web Services' chapter of the *Security Guide*.

Using the Web Services Registry Manager

Before you run `itws_registrymanager.bat` or `itws_registrymanager`, you must first modify the setting for `java_flags`.

The current setting is as follows:

```
set java_flags=--Djavax.xml.registry.ConnectionFactoryClass=
com.iona.uddi.v2.xml.registry.ConnectionFactoryImpl
-Djavax.net.ssl.trustStore=etc/certs/.truststore
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.protocol.handler.pkgs=com.sun.net.ssl.internal.www.protocol
```

You must reset this as follows:

```
set java_flags=-Djavax.xml.registry.ConnectionFactoryClass=
com.iona.uddi.v2.xml.registry.ConnectionFactoryImpl
-Djavax.net.ssl.trustStore
=$PRODUCT_DIR/etc/domains/$DOMAIN_NAME/certs/.truststore
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.protocol.handler.pkgs=com.sun.net.ssl.internal.www.protocol
```

Security

The security issues are as follows:

Creating a Domain with iS2 enabled

If you create a domain with the security service (iS2) enabled and you run any of the following consoles:

```
ittrader_console
itnotify_console
itlogging_console
```

You must pass it the following parameter:

```
-ORBname iona_utilities.admin
```

For example:

```
itnotify_console -ORBname iona_utilities.admin
```

Performance optimization for TLS servers

A reduction in TLS server-side performance may be apparent due to extra security checking that is related to the Important multiple listeners security warning for TLS servers.

However, this checking is not required for most applications and can be completely disabled when the criteria for safely doing so are met. These criteria are explained in Relevant applications.

In the next release or patch of Orbix 6.1, the ORB will automatically be able to determine if this check is required and will disable it automatically if not. Until then the default is more secure rather than faster.

Important multiple listeners security warning for TLS servers

This describes necessary precautions to prevent an attack on TLS servers that have multiple IIOP or IIOP/TLS listeners. This precaution is enforced automatically by default in Orbix 6.1. The user would have to take steps to disable this behavior.

Relevant applications This warning applies to the following:

- Advanced C++ and Java IIOP/TLS server applications that use security POA policies programatically to specify different security settings on a per POA basis.
- Client applications that serve callback objects—these types of clients are also servers.

This warning does not apply to the following:

- Applications that have been configured to be secure without code changes, or to applications that do not programatically use security related POA policies.
- Applications that have exactly the same security configuration for all POAs, or those that apply policies to only the ORB.

Consequences of a successful attack An attacker would be able to perform invocations on a POA that had certain strong security policies specified by attacking one of the less secure listening endpoints of the server. In other words, the security of your server would only be as strong as the security of the weakest POA in it.

Precautions By default, in Orbix 6.1 you must do nothing but ensure that you do not set the following variable to `""`. This variable has a default value that enables the `iiop_tls` plug-in to register an interceptor that performs listener endpoint compatibility checking to prevent this type of attack.

```
binding:server_binding_list_prefix = "";
```

Disabling the Listener compatibility checker for performance reasons It is valid to disable this check for most applications and some performance gain will be realized as a result.

If you have carefully identified that your applications is not susceptible to this attack by checking the Relevant applications, you can completely disable this extra check by setting the specified configuration variable as follows:

```
binding:server_binding_list_prefix = "";
```

| Security service on Windows and Linux | On Linux and Windows VC6.1, C++ CORBA servers and services being authenticated in a security service domain experience random crashes. The problem only occurs in the domains where the security service is deployed. |

Windows and Linux patches are available to fix this problem for SSL kits. Please contact support@iona.com for download details. To apply the patch, the relevant tar file should be copied into the IT_PRODUCT_DIR and untarred. The relevant libraries will be replaced.

If you have developed applications that link against the existing isp_c libraries, those applications should be relinked.

On Linux, you also need to change the libit_isp_c.so symbolic link in <IT_PRODUCT_DIR>/asp/6.1/lib to point to:

```
../../../shlib/libit_isp_c_gcc32.so.5
```

Applications that are not relinked will continue to run but may experience the random crash.

Notification service in a secure domain on Linux AS 3.0

To run the notification service on Red Hat Linux AS 3.0 in a secure domain without incident, you must set the LD_ASSUME_KERNEL environment variable prior to starting the services. LD_ASSUME_KERNEL should be set to 2.4.19 or earlier.

Setting LD_ASSUME_KERNEL to a kernel higher than 2.4.19 causes the notification service to fail when performing secured operations on that service.

A patch is available to fix this problem (same patch as "Security service on Windows and Linux"). Please contact support@iona.com for download details.

Unsupported IONA Security Framework features

The *Security Guide* contains information about security features that are provided in several IONA products. The following IONA Security Framework features are not currently supported in Orbix 6.1:

- Siteminder adapter.
- iS2 clustering.

The following IONA Security Framework feature is not included in your Orbix 6.1 Standard or Enterprise license:

- Support for developing custom iS2 server adapters.

Please contact your IONA account manager or IONA Customer Services for information on how to obtain a license for custom iS2 adaptor support.

Demos

The demos issues are as follows:

Codeset_Converter demo on HP-UX

On HP-UX, Orbix developer, an error in the makefile located in `$IT_PRODUCT_DIR/asp/6.1/demos/corba/orb/codeset_converter/plugin` prevents the `codeset_converter` demo from working when compiled with classic iostreams.

Replacing `SHLIB_NAME=libcccp_acca03331.5` in line 18 of the makefile with `SHLIB_NAME=libcccp_$(SHLIB_CXX_COMPILER_ID).5` and a subsequent rebuild fixes this problem.

Alternatively, you can rename the library and dependencies file built with classic iostreams from `libcccp_acca0331.5` to `libcccp_acca0331cios.5` and `libcccp_acca0331.5.dependencies` to `libcccp_acca0331cios.5.dependencies`.

Bugs Fixed in Orbix 6.1

The following bugs have been fixed in Orbix 6.1:

Bug	Description
12000793	Enhancement to Orbix Locator to allow clients to contact individual replica members in a cluster.
68552	COMet does not pick up value of configuration variable `TYPEMAN_IFR_IOR_FILENAME`.
68542	The COMet typestore ignores the values of `TYPEMAN_DISK_CACHE_SIZE` and `TYPEMAN_MEM_CACHE_SIZE`.
68498	Orbix2000 1.2.1 enhancement request to remove Java `yield()` calls.
68478	`itdeployer` fails if you install ASP6 SP3 in a directory where it's name includes -d or -D.
68449	Locator redirects clients' requests to a dead server in the round-robin load-balancing scheme.
68445	`_non_existent` returns `FALSE` when object does not exist.

Bug	Description
68436	Multiple `orb_inits` cause core dump in ASP 6.0.3 on Solaris.
68417	Deadlock in BiDir server.
68396	If the locator loses contact with a node daemon, it never discovers it again.
68374	Orbix ASP Java ORB's object reference `toString()` does not print the correct port number for port numbers above `32767`.
68370	ORB locks up when WorkQueue gets full.
68355	`-host`, `-hostnamePolicy` command line options in `itconfigure` have no effect when used with `nogui` mode without the `-save` option.
68337	ASP 6.x PDK missing some IDL files in kit.
68332	ASP 6.0.3 does not queue requests when the number exceeds the `high_water_mark`.
68329	`-libs`/`-L` flag for `itconfigure` does not work in GUI mode.
68324	Node daemon's process monitoring is broken with regards to scripts used to launch servers.
68298	ASP 6.0.3 `openssl.exe` requires `ssleay32.dll`, which is not shipped with the product.
68285	ASP 6.x `itconfigure` depends on files from the J2EE runtime.
68253	Node daemon core dumps when activator tries to launch a process that does not exist, that is, the path name is invalid.
68241	ASP 6 multithreading CORBA application—connection establishment and method invocation takes a long time in a thread, if there are other threads trying to establish connections to non-existing servers.
68233	Closed Listener in ATLI2 never re-tried in a C++ implementation.

Bug	Description
68232	ASP 6.0.1 `itconfigure` should take care of `product_dir` environment variable more robustly.
68208	ASPv6.0 SP2 Java implementation of Dynamic Array's, Dyn Sequence, and Dyn Struct uses equals instead of equivalent.
68189	Enhancement request to be able to dynamically reconfigure the logging levels of IONA services.
68187	Requests do not get queued when the `thread_pool:high_water_mark` is reached in JAVA ATLI2 in Orbix 6.0.2.
68155	ASP6.0 SP2 Web Services Builder fails to start when run in a secure only domain. Throws `NullPointerException`.
68154	IP address is stored in SSL as part of the IOR.
68133	Problem running `itadmin ns list` on ASP 6.0.2.
68078	Enhancement request to add more logging to the core ASP services.
67958	Locator's internal cache of IORs can go stale if the local node daemon is killed.
67707	Setting the `high_water_mark` to unlimited causes a hard-wired limit of `500` to be used.
67136	A TLS secure client should be able to use a `corbaloc` string to call a server.
66499	Enhancement request for `itconfigure` tool for Orbix 2000.
58582	Enhancement request for TLS smart card support in Orbix 2000.

Platforms/Features Not Supported in Next Release (Orbix 6.2)

The following platforms and features will not be supported in the Orbix 6.2 release:

- Classic I/O streams will no longer be available on HP-UX/PA-RISC.
- Red Hat Linux 7.2 will be replaced by Red Hat Enterprise Linux AS 3.0.
- Gcc 3.2.2 on Linux will be replaced by Gcc 3.3.3.
- Windows NT will be replaced by Windows 2003.

Documentation Updates

The online documentation includes the following updates, published after the Orbix 6.1 Documentation CD was released:

- "Release Notes".
- "Installation Guide".
- "Security Guide".
- "Enterprise Messaging Guide Java Edition".

The latest updates to the Orbix documentation can be found at
http://www.iona.com/support/docs/orbix/6.1/index.xml

Release Notes

This document includes the following updates to the *"Known Issues"*:

- Notification service in a secure domain on Linux AS 3.0.
- Codeset_Converter demo on HP-UX.
- itconfigure on SuSE Linux.
- Unsupported IONA Security Framework features.
- Uppercase or mixed case hostnames.

Installation Guide

The *Installation Guide* includes the following updates:

- *The* "*Prerequisites*" section includes new support for SuSE Linux 8 and Redhat Linux AS 3.0.
- The "*C++ Development Environment Requirements*" section includes new Windows 2000 support for Visual Studio .NET 2003 (VC7.1).
- The "*Installing with the GUI*" section includes additional instructions for installing on Redhat Linux AS.

Security Guide

The *Security Guide* includes the following updates:

- Some technical corrections were made to the "*Hints for Setting Association Options*" section in Chapter 11.
- The section on the SiteMinder adapter was removed. This is not supported at the moment.
- All references to iS2 clustering were removed from the appendices. This feature is not yet implemented in Orbix.

Enterprise Messaging Guide Java Edition

Chapter 4, "*Developing Suppliers and Consumers*" includes a code example that has been updated with technical corrections: Example 5, "*Creating a Structured Message*".

Reporting Problems

Contact customer support at http://www.iona.com/support/contact/

Other Resources

- Knowledge Base articles
  (`http://www.iona.com/support/knowledge_base/index.xml`) provide a
  database of practical advice on specific development issues, contributed by
  IONA developers, support specialists, and customers.
- IONA University (`http://www.iona.com/info/services/ps/`) delivers
  practical and insightful courses that cover technical and product issues as
  well as standards-based best practices gleaned from real-world projects.
- IONA Professional Services
  (`http://www.iona.com/info/services/consulting/`) provide product
  expertise and consulting solutions that empower end-users, system
  integrators and software vendors with the knowledge to fully leverage Orbix
  6.1. Together, IONA consultants and Orbix 6.1 equip you with a single
  platform for integrating and developing extremely reliable, scalable and
  secure e-Business systems.
- IONA security bulletins are available as part of our customer warning
  system. To receive these bulletins, please subcribe to the
  `security-alert@iona.com` mailing list.

  To subscribe send an email to `listserver@iona.com`. Leave the email
  Subject field blank and, in the body of the email, type:

  subscribe security-alert <your email address>

  To unsubscribe do the same, but type unsubscribe in the body of the email.
  Note: Please do not try to post queries to this email alias; it has not been
  set up to receive queries.